IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: CARROLL, Nicholas M.
Application No.: 10/710,491 Group No.: 2137
Filed: 07/15/2004 Examiner: WILLIAMS, Jeffery L
For: SYSTEM FOR PROTECTING DOMAIN SYSTEM CONFIGURATIONS FROM USERS WITH LOCAL PRIVILEGE RIGHTS

Mail Stop Appeal Briefs-Patents
Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450

APPEAL BRIEF (37 C.F.R. § 41.31)

This brief is in furtherance of the Notice of Appeal, filed herewith.

The fees required under § 41.20 for filing both the Notice and this Brief are dealt with in the Office's EFS-Web system along with the filing of these documents.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(1)):

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST
(37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is Lieberman Software Corporation, a California corporation of 1900 Avenue of the Stars, Suite 425, Los Angeles, California 90067, which is assignee of the entire right, title and interest to the invention in the United States and in all foreign countries.

II RELATED APPEALS AND INTERFERENCES
(37 C.F.R. § 41.37(c)(1)(ii))

With respect to other appeals or interferences which may be related to, that will directly affect, or be directly affected by or have a bearing on the Board's decision in this appeal, there are no such appeals or interferences.

III STATUS OF CLAIMS
(37 C.F.R. § 41.37(c)(1)(iii))

The status of the claims in this application are:

A. TOTAL NUMBER OF CLAIMS IN THE APPLICATION

Claims in the application are: 1-30

B. STATUS OF ALL OF THE CLAIMS

1. Claims rejected: 1-30
2. Claims allowed or confirmed: NONE
3. Claims withdrawn from consideration: NONE
4. Claims objected to: NONE
5. Claims canceled: NONE
6. Accordingly, the pending claims are: 1-30

C. CLAIMS ON APPEAL

The claims on appeal are: 1-30

IV STATUS OF AMENDMENTS
(37 C.F.R. § 41.37(c)(1)(iv))

Insofar as understood by the appellant, all amendments have been entered.

V SUMMARY OF CLAIMED SUBJECT MATTER
(37 C.F.R. § 41.37(c)(1)(v))

Large organizations typically employ large-scale computer networks, or intranets, consisting of many computers all interconnected to a variety of servers and data sources. For example, Windows (TM) based systems are frequently organized in such intranets into "domains": a group of many systems under the supervision of a single (or multiple) domain controller(s). This allows a system administrator to make domain-wide changes to the configuration of the individual machines, all from a single location. (paragraph [0002])

FIG. 1 (background art) depicts a common implementation of this. A single user group is established on the domain controller(s), known as the "Domain Administrators Group," and it is ensured that this group is a member of another group (typically the Local Administrators Group") with local privileges on each individual workstation being managed. ([0003]) It is also common, however, to permit individual users in a domain to be members of the Local Administrators Groups of their own individual computers, thus allowing them to install software packages and perform minor maintenance without the need for intervention by a system administrator. ([0004])

Unfortunately, allowing individual users to be members of the Local Administrators Group can also lead to undesirable consequences. These users are sometimes untrained, ill advised, or simply act out of malice when performing changes locally. For instance, they can undo configuration changes made by the system administrators and they can even remove the Domain Administrators Group from the Local Administrators Group, thus preventing domain administrators from making changes on the local machine. ([0005])

As recited in independent claims 1, 11, and 21, Appellants' invention comprises novel methods, articles, and systems for protecting domain system configurations from users with local privilege rights.

Turning first to claim 1, this recites a method wherein the preamble recites relevant aspects of the applicable environment or "work piece" and the body of the claim recites three major steps.

The preamble states that this is a "method for protecting the configuration of a securable object in an operating system." A securable object is what its label implies, and this may be an entirely conventional element (albeit one operated on by the invention in an unconventional

manner, as described presently). A securable object an object that can be secured by use of the computer operating system. ([0026])

Additionally, the preamble of claim 1 states that this is "wherein a security descriptor for the securable object includes a discretionary access control list (DACL)." This security descriptor may also be conventional. A security descriptor basically stores information about an owner of an object and what permissions that "owner" has granted to others ([0037]). See also, [0026] through [0036], which discuss security descriptors further and present examples in a number of tables. The discretionary access control list (DACL) here may also be conventional. Of particular relevance in this appeal, however, it should be noted that a DACL is a special "permissions" type of access control list (ACL) and not merely any ACL. ([0038] and [0047]) Basically, ACLs can be classified as discretionary and mandatory, and a system is said to have discretionary access control if the creator or owner of an object can fully control access to the object (a more full definition of this and its source are provided in the arguments below).

The steps of the method in claim 1 work with the just described preamble elements. The first step is to make a copy of the security descriptor (the one for the securable object of interest). This is included in step 116 in the example in FIG. 2.

The second step is adding a new access control entry (ACE) to the DACL in this copy (see e.g., step 116 in FIG. 2). In particular, however, this added ACE is one that denies the locally privileged group an access right to the securable object. A key point to grasp therefore here is that the added ACE is used unconventionally, not to add a permission in the conventional manner, but instead to explicitly deny a particular permission.

And the third step is to overwrite the original security descriptor in the operating system with this altered ACE copy (see e.g., step 118 in FIG. 2). The way in which an affected group is stored by the operating system now particularly assists the invention. The information for user groups in NT-class systems (for example) is stored as keys in the protected area of the system registry. Because the security system in NT-class systems handles all security descriptors identically, it applies the "set value" action ACE to the registry key despite the fact that the registry key in this case represents a user group. The subtle but powerful result of this is that, once the modified DACL is written to the system, any member of the locked-out group is then unable to modify the values stored in the registry key that describes that group and any attempt to modify the group's permissions, contents, etc. will fail when the system tries to make the

change to the registry keys holding the information. ([0052]-[0054]) Another benefit of this is that the change will effectively be invisible to the affected users, because they will not be able to see their membership in the locked-out groups. ([0024])

Turning next to dependent claims 2 and 3, these recite earlier steps than those in claim 1. Specifically claim 2 adds identifying the particular security descriptor needed (see e.g., steps 106 and 108 in FIG. 2) and determining if a change is even needed (step 110). The particular security descriptor of interest may already be identified or doing so may simply be straightforward, so this is not an appropriate limitation the needs to appear in claim 1. Claim 3 adds determining if a change is needed, that is, if the group is already locked out. Cumulatively adding new ACEs with redundant effect can burden the system as it resolves a DACL, but avoiding this is also not necessary and it also is not a limitation of claim 1. ([0042]-[0051])

Turning next to dependent claim 7, this essentially recites claim 1 but applied now to all local groups (please note, groups plural). For this, each ACEs (as already recited in parent claim 1, only now one having one for each of the groups) is copied, altered and stored.

Moving on to claim 11, this recites a computer program, embodied on a computer readable storage medium, for performing essentially the steps of claim 1. The Examiner has taken the position that claim 11 and its dependent claims 12-20 can be treated similarly to claims 1-10. That is acceptable to Appellant.

And moving on to claim 21, this recites a system for performing essentially the steps of claim 1. The Examiner has taken the position that claim 21 and its dependent claims 22-30 can be treated similarly to claims 1-10. That is also acceptable to Appellant.

Additionally, even though there are no issues with respect to this raised by the Examiner, we point out that claims 21-30 recite means plus function limitations and we now discuss aspects of this that may, arguably, be appropriate in view of the Office's rules for such subject matter that is in any case that is under appeal in any respect.

Claim 21 corresponds closely with claim 1. Accordingly, steps 116 and 118 in FIG. 2 also show the structure, material, and acts that are relevant to claim 21. Specifically, step 116 corresponds with the means for making a copy and the means for adding in claim 21; and step 118 corresponds with the means for overwriting in claim 21. Paragraph [0061] explicitly

discusses step 116 and [0062] explicitly discusses step 118. Paragraphs [0026] through [0038], and [0047] also generally discuss the means for making a copy and the means for adding in claim 21; and [0052]-[0054] also generally discuss the means for overwriting in claim 21.

Claim 22 corresponds closely with claim 2, reciting a means for determining. Step 106 in FIG. 2 shows the structure, material, and acts that are relevant to this means for determining; [0056] specifically discusses this; and [0042]-[0051] generally discuss this.

Claim 23 corresponds closely with claim 3, reciting a means for examining. Step 110 in FIG. 2 shows the structure, material, and acts that are relevant to this means for examining; [0059] specifically discusses this; and [0042]-[0051] also generally discuss this.

Claim 24 corresponds closely with claim 4, reciting a means for providing. Step 116 in FIG. 2 shows the structure, material, and acts that are relevant to this means for providing; [0051] specifically discusses this; and [0042]-[0050] also generally discuss this.

Claim 27 corresponds closely with claim 4, reciting that the means that adds of claim 21 here further does so to affect all local groups. FIG. 1 shows local versus remote groups and [0025] specifically discuss this limitation.

Claim 30 is unique, merely reciting a structural imitation that all of the means of parent claim 21 are comprised within a single tool. FIG. 2 shows a group change lockout process (GLP 100), that can be viewed as a whole or as its sub-steps. It follows that what is shown here can be done with as little as the single GLP 100 and, even if these were not the case, it will be readily appreciated by those of ordinary skill in the art that such a GLP 100 can be embodied is one tool rather than as multiple tools.

Finally, claims 25-26 and 28-29 do not recite additional means plus function limitations, and Appellant urges that no particularized discussion of these claims with respect to means plus function is appropriate or possible.

VI GROUND OF REJECTION TO BE REVIEWED ON APPEAL
(37 C.F.R. § 41.37(c)(1)(vi))

A. Whether claims 1-30 are anticipated by U.S. Pat. App. No. 2004/0215650 by et al. (herein after "Shaji"), and thereby unpatentable under 35 U.S.C. § 102(e).

B. Whether claims 21-30 are directed to non-statutory subject matter, and thereby unpatentable under 35 U.S.C. § 101.

C. Whether claims 7, 9, 17, and 27 are indefinite, and thereby unpatentable under 35 U.S.C. § 112, second paragraph.

VII ARGUMENT

(37 C.F.R. § 41.37(c)(1)(vii))

VII(A) ARGUMENTS—REJECTIONS UNDER 35 U.S.C. § 102

Appellants position here is that a *prima facie* case for anticipation has not been made and, in the alternative, that any such case that might be inferred from the Examiner's limited remarks in the Actions will be a case that is not supportable by the cited reference. We show below that the Actions have failed to show that any of the major limitations of Appellant's claims, much less all of them, are taught by the cited reference.

Regarding claim 1, both the 08/03/2007 Action, at pg. 4-5, and the 01/16/2008 Action, at pg. 4, state "minimal" rejections of claim 1. These are minimal in that the Examiner merely recites portions (not even all) of claim 1 and adds parenthetical listings of paragraph numbers in Shaji where he apparently feels that this reference teaches something relevant. Basically, the Examiner has not even bothered to articulate a prima facie case for this rejection.

For example, the Actions states that "Shaji discloses: making a copy of the security descriptor (par. 18, 91)." However, [0018] and [0091] of Shaji do not support the implicit assertion here. To the extent that any security descriptor is "copied" here in Shaji, this is not applicable to the relevant context. As is well known to artisans in this field, many things in an operating system can have security descriptors. The only one that is relevant here, however, is "a security descriptor for the securable object" and further that this securable object be one that "includes a discretionary access control list (DACL)" (claim 1). There are no arguments in the record that Shaji teaches these. Accordingly, the Action fails to state a prima facie case based on Shaji. More importantly, we urge that Shaji simply cannot support a prima facie case for anticipation here because it simply does not anywhere teach a security descriptor that is equivalent to Appellant's as recited in the claims.

In the 01/16/2008 Action at pg. 7, item iii (in the Response to Arguments) the Examiner has replied to some of our above points. With respect to a discretionary access control list (DACL) his counter arguments here is a semantic one. Essentially, the Examiner argues that Shaji does teach access control lists (ACLs); that an ACL list can be changed; therefore Shaji

teaches DACLs. This is error in multiple respects. Shaji nowhere teaches or discusses a discretionary access control list, and it does not use the word "discretionary" anywhere. As discussed in Appellant's specification at [0038], a DACL is a special form of ACL having a meaning as industry standard terminology. The Examiner thus overlooks or ignores what is well known in this art and is verifiable by reference to any number of industry accepted references. For example:

> Systems that use ACLs can be classified into two categories: discretionary and mandatory. A system is said to have discretionary access control if the creator or owner of an object can fully control access to the object, including, for example, altering the object's ACL to grant access to anyone else. A system is said to have mandatory access control (also known as "non-discretionary access control" in the security literature) if it enforces system-wide restrictions that override the permissions stated in the ACL. *Wikipedia.org "access control list"*

If the Examiner feels that an ACL is equivalent to a DACL in a manner that is relevant to claim 1, the Examiner should have at least articulated a reasoning for this for the record and provided Appellant a reasonable opportunity to reply. However, the Examiner simply has not done this and there similarly is nothing in the record explaining why the Examiner feels that Shaji teaches any of the DACL related/specific limitations recited in claim 1.

Continuing with respect to claim 1, the Actions also state that [Shaji discloses] "adding a new access control entry (ACE) to the DACL in said copy, wherein said new ACE specifies denying the locally privileged group an access right to the securable object (par. 18, 19, 89)" (underline emphasis added). However, as discussed above, there is no showing that Shaji teaches a DACL (for a securable object in an operating system or even for anything). In fact, in [0018] and [0019] Shaji also does not teach an access control entry (ACE). If Shaji did, it would presumably have used the industry standard term "access control entry" or the industry standard acronym "ACE," as it does elsewhere, including [0089]. As for [0089], this is merely a recitation of entirely conventional ACE characteristics. Shaji nowhere teaches denying anything that is relevant to this matter, especially not by using a new ACE, or denying something to a locally privileged group, and not to all of these also with the other limitations recited in claim 1.

In the 01/16/2008 Action at pg. 8, item iv (in the Response to Arguments) the Examiner has also replied to some points here. Basically, the Examiner now argues; 'oh, this is not in the

previously cited paragraphs of Shaji, but it is there somewhere' and the Examiner now cites [0001] through [0123] -- all of Shaji, every single paragraph of its specification.

Continuing further with respect to claim 1, the Actions also state that [Shaji discloses] "overwriting the security descriptor in the operating system with said copy (par. 18)." However, in [0018] Shaji merely teaches loading and mapping to a security descriptor. It teaches nothing here about overwriting a security descriptor, and especially not about doing so with a copy as prepared in accord with the limitations in the preceding step in claim 1.

In the 01/16/2008 Action at pg. 9, item v (in the Response to Arguments) the Examiner has also replied to this. Here the Examiner "points out that the prior art clearly discloses ... (i.e., [SIC] see cited portions of prior art, or surrounding portions." So the Examiner's argument again is that support for the rejection is there somewhere in the entirety of Shaji, but he apparently cannot identify where.

In sum, Shaji does not teach any of the limitations of claim 1 that the Actions assert it teaches. Shaji certainly does not teach all of the limitations of Applicant's claim 1 and this claim should therefore be allowed.

Regarding claim 2, it should be allowed for at least the same reasons as parent claim 1. The Actions here further state "Shaji discloses: determining the relative identifier (RID) of the securable object; and finding the security descriptor for the securable object based on said RID (par. 13, 64)." However, the cite here also does not support the implied assertion here. For example, the cited paragraphs do not teach a relative identifier (RID), much less one used in the specific manner recited in the claim.

In the 01/16/2008 Action at pg. 9, item vi (in the Response to Arguments) the Examiner has also replied to this, by simply reiterating that [0013] and [0064] do disclose a relative identifier (RID) and stating that "Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention." First, [0013] and [0064] simply do not teach what the Examiner argues they teach this is an easily verifiable fact. Second, Appellant's point was and again is that the Examiner has not stated a *prima facie* case to support this rejection, and Appellant by pointing out specific error in the

Examiner's support for the rejection here (i.e., that the cited portions of the reference do not contain what the Examiner implies they do) is much more than a mere general allegation that claim 2 is patentable.

Regarding claim 3, it should also be allowed for at least the same reasons as parent claim 1. The Action here further states "Shaji discloses: further comprising examining the DACL to discover whether said access right is already denied (par. 18)." However, we have shown above that Shaji does not teach DACLs, and the [0018] of Shaji clearly does not teach "examining" and "discovering" steps related to such.

In the 01/16/2008 Action at pg. 10, item vii (in the Response to Arguments) the Examiner's reply to this is ridiculous. Among other things the Examiner here argues "that the features [steps for examining and discovering] upon which applicant relies ... are not recited in the rejected claim(s)." The Examiner is clearly wrong. Claim 3 recites "The method of claim 1, further comprising examining the DACL to discover whether said access right is already denied" (underline emphasis added).

Regarding claim 5, it should also be allowed for at least the same reasons as parent claim 1. The Actions here further state "Shaji discloses: wherein the securable object is a group other than the local administrators group (par. 4)." In reply, Applicant has argued "[a]s is well known in the art, groups categorize securable objects (e.g., membership in a group, or the absence there of, defines the access rights to a securable object)." This argument stands un-rebutted, even though the Examiner does make other comments in the 01/16/2008 Action at pg. 10, item ix (in the Response to Arguments).

Regarding claim 7, it should also be allowed for at least the same reasons as parent claims 6, 5, and 1. The Actions here further state "Shaji discloses: wherein said domain administrator group is a remotely hosted group, and the method further comprising adding said new ACEs to the DACL in said copy to deny all local groups said access right to the securable object (par. 4,5,47)." However, we have shown above that Shaji does not teach a DACL. Furthermore, although [0004], [0005], and [0047] are newly cited here, they also do not teach DACLs, and particularly not such as subject to the other limitations recited in claim 7.

These argument stand un-rebutted to date (being unmentioned even in the Response to Arguments in the 01/16/2008 Action).

Regarding claims 4, 6, and 8-10, these should also be allowed for at least the same reasons as their parent claims.

Regarding claims 11-30, the Actions state (e.g., the 01/16/2008 Action at pg. 6) that "they comprise essentially similar recitations [as claims 1-10]." Appellant agrees, and urges now that they are therefore allowable for at least the same reasons discussed above.

VII(B) ARGUMENTS—REJECTIONS UNDER 35 U.S.C. § 101

Claim 21, and its dependent claims 22-30, are rejected as being directed to non-statutory subject matter. The Examiner has wrongly held that these claims "comprise a computer program" (01/16/2008 Action, pg. 2), whereas claim 21 actually recites a "system for protecting the configuration of a securable object in an operating system of a computer ...." The Examiner's stated rationale for this rejection is that claim 21 recites a "system" and that "the words "system" and "machine" are not equivalents" (01/16/2008 Action, pg. 6).

First, this is hypercritical examination based on semantics and ignores the relevant context of the subject matter. As such, the Examiner here is merely making what the Office itself terms a "technical rejection" and describes as improper in MPEP § 706.03.

Second, this would deny Appellant the right to be their own lexicographer and to write the claims is they deem appropriate (in conflict with MPEP §§ 706.03(d) and 2111.01 (IV)). Note, the Examiner has not argued that claims 21-30 are indefinite under 35 U.S.C. 112, or that he does not understand these claims, or that one of ordinary skill in the art would not understand these claims.

Third, this is capricious, apparently being done merely out of idiosyncratic preference and it is even inconsistent on the part of this particular Examiner. For example, the Examiner must certainly know that "apparatus" is also not one of the four specifically enumerated statutory categories, yet he has allowed patent claims that recite an "apparatus" (see e.g., U.S. Pat No.

7,096,359 and 6,922,782). Furthermore, even within this application, the Examiner has not objected to claim 1-10 reciting a method, whereas the statute uses the term "process."

Fourth and fifth, this simply does not comport with the procedures of the Office or the law. If rigid recitation of a statutory category was a requirement of the Office it would not bother guiding us with MPEP § 2106 (IV)(B) (Patent Subject Matter Eligibility; Determine Whether The Claimed Invention Complies With 35 U.S.C. 101; Determine Whether the Claimed Invention Falls Within An Enumerated Statutory Category), and this guidance would not cite important case law including the following:

> The question of whether a claim encompasses statutory subject matter should not focus on which of the four categories of subject matter a claim is directed to -- process, machine, manufacture, or composition of matter -- [provided the subject matter falls into at least one category of statutory subject matter] but rather on the essential characteristics of the subject matter, in particular, its practical utility. *(underline emphasis added) State Street Bank & Trust Co. v. Signature Financial Group Inc., 149 F.3d 1368, 1375, 47 USPQ2d 1596, 1602 (Fed. Cir. 1998)*

Please note, the Examiner has never argued that Appellant's claimed subject matter lacks practical utility.

VII(C) ARGUMENTS—REJECTIONS UNDER 35 U.S.C. § 112, SECOND PARAGRAPH

Claims 7, 9, 17, and 27 are rejected as being indefinite. The Examiner wrongly feels that these claims lack antecedent basis for "said new ACEs" (01/16/2008 Action, pg. 3).

Claim 7 has been argued in the record as an example. It recites "adding said new ACEs to the [discretionary access control list] DACL in said copy to deny all local groups said access rights" *(underline emphasis added here)*. Claim 7 depends from claim 1, which recites "adding a new access control entry (ACE)" that controls access by a local group. There thus is antecedent basis in claim 7 for at least "said new ACE" with respect to one local group. The flaw in the Examiner's reasoning here is that it overlooks that claim 7 recites "local groups" -- plural, that there then will be a said new ACE for each local group, and that a plurality of such will then be added to the DACL. As one of ordinary skill in the art will generally know, and as discussed in Applicant's specification at [0002]-[0006] and [0065], it is overwhelmingly the case in actual operating systems today that there are many local groups (which was the reason Appellant

drafted claim 7 to recite groups plural). Accordingly, "said new ACEs" as recited in claim 7 has antecedent basis, is grammatically correct, and is recited in the manner best understandable to one of ordinary skill in the art.

The Examiner has argued that clams 9, 17 and 27, should be treated the same as claim 7. We agree, albeit to arrive at a different conclusion.

VIII CLAIMS APPENDIX
(37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal are:

1. A method for protecting the configuration of a securable object in an operating system from members of a locally privileged group, wherein a security descriptor for the securable object includes a discretionary access control list (DACL), the method comprising:

making a copy of the security descriptor;

adding a new access control entry (ACE) to the DACL in said copy, wherein said new ACE specifies denying the locally privileged group an access right to the securable object; and

overwriting the security descriptor in the operating system with said copy.

2. The method of claim 1, further comprising:

determining a relative identifier (RID) of the securable object; and

finding the security descriptor for the securable object based on said RID.

3. The method of claim 1, further comprising examining the DACL to discover whether said access right is already denied.

4. The method of claim 1, wherein said new ACE is added as a first ACE in the DACL.

5. The method of claim 1, wherein the securable object is a group other than a local administrators group.

6. The method of claim 5, wherein said group is a domain administrator group.

7. The method of claim 6, wherein said domain administrator group is a remotely hosted group, and the method further comprising adding said new ACEs to the DACL in said copy to deny all local groups said access right to the securable object.

8. The method of claim 5, wherein said access right includes a right to change permissions of said group.

9. The method of claim 7, wherein said access right also includes a right to view permissions of said group.

10. The method of claim 1, wherein a single software tool performs the method.

11. A computer program, embodied on a computer readable storage medium, for protecting the configuration of a securable object in an operating system from members of a locally privileged group, wherein a security descriptor for the securable object includes a discretionary access control list (DACL), the computer program comprising:

a code segment makes a copy of the security descriptor;

a code segment that adds a new access control entry (ACE) to the DACL in said copy, wherein said new ACE specifies denying the locally privileged group an access right to the securable object; and

a code segment that overwrites the security descriptor in the operating system with said copy.

12. The computer program of claim 11, further comprising:

a code segment that determines a relative identifier (RID) of the securable object; and

a code segment that finds the security descriptor for the securable object based on said RID.

13. The computer program of claim 11, further comprising a code segment that examines the DACL to discover whether said access right is already denied.

14. The computer program of claim 11, further comprising a code segment that provides that said new ACE is added as a first ACE in the DACL.

15. The computer program of claim 11, wherein the securable object is a group other than a local administrators group.

16. The computer program of claim 15, wherein said group is a domain administrator group.

17. The computer program of claim 16, wherein said domain administrator group is a remotely hosted group, and said code segment that adds further adds said new ACEs to the DACL in said copy to deny all local groups said access right to the securable object.

18. The computer program of claim 15, wherein said access right includes a right to change permissions of said group.

19. The computer program of claim 18, wherein said access right also includes a right to view permissions of said group.

20. The computer program of claim 11, wherein all said code segments are part of a single software tool.

21. A system for protecting the configuration of a securable object in an operating system of a computer from members of a locally privileged group, wherein a security descriptor for the securable object includes a discretionary access control list (DACL), the system comprising:

means for making a copy of the security descriptor;

means for adding a new access control entry (ACE) to the DACL in said copy, wherein said new ACE specifies denying the locally privileged group an access right to the securable object; and

means for overwriting the security descriptor in the operating system of the computer with said copy.

22. The system of claim 21, further comprising:

means for determining a relative identifier (RID) of the securable object; and

means for finding the security descriptor for the securable object based on said RID.

23. The system of claim 21, further comprising means for examining the DACL to discover whether said access right is already denied.

24. The system of claim 21, further comprising means for providing that said new ACE is added as a first ACE in the DACL.

25. The system of claim 21, wherein the securable object is a group other than a local administrators group.

26. The system of claim 25, wherein said group is a domain administrator group.

27. The system of claim 26, wherein said domain administrator group is a remotely hosted group, and said means that adds further adds said new ACEs to the DACL in said copy to deny all local groups said access right to the securable object.

28. The system of claim 25, wherein said access right includes a right to change permissions of said group.

29. The system of claim 28, wherein said access right also includes a right to view permissions of said group.

30. The system of claim 21, wherein said means are comprised within a single software tool.

IX EVIDENCE APPENDIX

(37 C.F.R. § 41.37(c)(1)(ix))

None.

X RELATED PROCEEDINGS APPENDIX

(37 C.F.R. § 41.37(c)(1)(x))

None.

Patent Venture Group
10788 Civic Center Drive, Suite 215
Rancho Cucamonga, California 91730-3805

Telephone: (909) 758-5145
Facsimile: (888) 847-2501

Respectfully Submitted,

Raymond E. Roberts
Reg. No.: 38,597